UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/713,560 | 11/14/2003 | Richard Bussiere | ENI-037 | 8242 |

35557 7590 12/11/2006

CHRIS A. CASEIRO
VERRILL DANA, LLP
ONE PORTLAND SQUARE
PORTLAND, ME 04112-0586

| EXAMINER | |
|---|---|
| SZYMANSKI, THOMAS M | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2134 | |

DATE MAILED: 12/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/713,560 | BUSSIERE ET AL. | |
| | Examiner | Art Unit | |
| | Thomas Szymanski | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *06 October 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-27 have been examined.

### *Response to Arguments*

2. Applicant's arguments filed 10/06/2006 have been fully considered but they are not persuasive.

3. In reference to the applicant's assertions that Huff is inapplicable because Huff allegedly teaches the use of software based agents, the examiner directs applicant's attention to Huff page 10 line 19- page 11 line 5, which clearly denotes that the systems of Huff are implemented in hardware, software, or any combination thereof. The applicant is directed to MPEP 2123 which is provided below as a showing that although the teachings of Huff in relation to a hardware implementation may not be a preferred embodiment of that system it is nonetheless still taught by Huff and thus anticipates the applicant's claims.

MPEP 2123 states:

"I. PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN

"The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)).

A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments. Merck & Co. v. Biocraft Laboratories, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), cert. denied, 493 U.S. 975 (1989). See also > Upsher-Smith Labs. v. Pamlab, LLC, 412 F.3d 1319, 1323, 75 USPQ2d 1213, 1215 (Fed. Cir. 2005)(reference disclosing optional inclusion of a particular component teaches compositions that both do and do not contain that component);< Celeritas Technologies Ltd. v. Rockwell International Corp., 150 F.3d 1354, 1361, 47 USPQ2d 1516, 1522-23 (Fed. Cir. 1998) (The court held that the prior art anticipated the claims even though it taught away from the claimed invention. "The fact that a modem with a single carrier data signal is shown to be less than optimal does not vitiate the fact that it is disclosed.").

II. NONPREFERRED AND ALTERNATIVE EMBODIMENTS CONSTITUTE PRIOR ART

Disclosed examples and preferred embodiments do not constitute a teaching away from a broader disclosure or nonpreferred embodiments. In re Susi, 440 F.2d 442, 169 USPQ 423 (CCPA 1971). "A known or obvious composition does not become patentable simply because it has been described as somewhat inferior to some other product for the same use." In re Gurley, 27 F.3d 551, 554, 31 USPQ2d

1130, 1132 (Fed. Cir. 1994) (The invention was directed to an epoxy impregnated fiber-reinforced printed circuit material. The applied prior art reference taught a printed circuit material similar to that of the claims but impregnated with polyester-imide resin instead of epoxy. The reference, however, disclosed that epoxy was known for this use, but that epoxy impregnated circuit boards have "relatively acceptable dimensional stability" and "some degree of flexibility," but are inferior to circuit boards impregnated with polyester-imide resins. The court upheld the rejection concluding that applicant's argument that the reference teaches away from using epoxy was insufficient to overcome the rejection since "Gurley asserted no discovery beyond what was known in the art." 27 F.3d at 554, 31 USPQ2d at 1132.). Furthermore, "[t]he prior art's mere disclosure of more than one alternative does not constitute a teaching away from any of these alternatives because such disclosure does not criticize, discredit, or otherwise discourage the solution claimed...." In re Fulton, 391 F.3d 1195, 1201, 73 USPQ2d 1141, 1146 (Fed. Cir. 2004)."

4. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., solely hardware implementation, no IDS within end nodes) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The applicant's own disclosure suggests the implementation of the claimed invention as a combination of both hardware and/or software as alluded to in the following passages of the applicant's disclosure:

"The DIRS of the present invention interacts with, and enables acting upon information from, an IDS or intrusion detection function, whether that function is established in **hardware, firmware, software, or any combination thereof,** for network monitoring. (For purposes of this invention, an intrusion of the network infrastructure may enter the network infrastructure from an attached function or it may be generated within the network infrastructure.) One example of a suitable intrusion detection function is the Dragon.TM. Intrusion Defense System offered by Enterasys Networks, Inc., of Andover, Mass. The intrusion detection function must be able to detect and report identified occurrences deemed by the network administrator to be network security threats. The DIRS may operate through a policy manager function, which function may be established in **hardware, firmware, software or any combination thereof**, directly or indirectly connected to the intrusion detection function and configured to regulate network infrastructure device policies. "

"The information providing, policy assignment, and enforcement functions may include algorithms and processes necessary to identify information about attached functions and devices, provide that information, enforce sets of assigned policies, and make decisions regarding assigned policies. Module 108 can be implemented in **hardware and/or software.** For example, **particular software, firmware, or microcode functions executing on the network infrastructure devices can provide the information providing functions, policy enforcement as presently available in network infrastructure devices, and policy assignment decision making**. Alternatively, or in addition, hardware modules, such as programmable arrays or ASICs, can be used in the devices to provide some or all of those capabilities.

Further, the intrusion detection function may be implemented by any commercially available IDS, including the Dragon.TM. Intrusion Defense System provided by Enterasys Networks, Inc. of Andover, Mass. While the IDS may be a standalone appliance, it may alternatively be embodied in part or in full in one or more other devices of the network infrastructure 101"

5. The applicant has further argued that Huff does not teach implementation of the agents within the context of "network infrastructure" which is a defined in the applicant's disclosure as:

"A network permits communication or signal exchange among the various computing systems of the common group in some selectable way. The interconnection of those computing systems, as well as the devices that regulate and facilitate the exchange among the systems, represent a network. Further, networks may be interconnected together to establish internetworks. For purposes of the description of the present invention, the devices and functions that establish the interconnection represent the network infrastructure."

From this disclosure by the applicant it is clear that the infrastructure/signaling devices relate to such devices as switches, routers, firewalls, access points, MANs, WANs, voice interconnect systems, VPNs, address resolution servers, etc all of which are well known to be comprised of either software, and/or hardware and furthermore from the disclosure of Huff are anticipated. Specifically, Huff states at page 8 lines 10-14, 20-30, that such devices as servers, and all other addressable nodes contain the agent functionality. The qualifier for a device to include the agent functionality of Huff is simply that the device be an addressable node, as it is well known within the art such devices as routers, switches, and VPNs are all network addressable elements. Furthermore, such devices as vpns and firewalls are well known to be analogous with servers as recited by Huff.

"...a plurality of network devices on which an embodiment of the invention may be implemented. The network devices include devices such as hosts, **servers**, and personal computers. ...As can be appreciated, many other devices can be coupled to the network including additional personal computers,

mini-mainframes, mainframes, and other devices not illustrated or described which are well known in the art" - Huff page 8.
The examiner maintains that such devices as switches and routers are some of the most highly well known devices in the art and thus are clearly part of the intrusion detection system of Huff as outlined above since these devices are clearly fall within the scope of the description of Huff of servers and all network addressable nodes. It is the examiner's recommendation that if the structures of the applicant's system and that of Huff actually do differ that the claim language be specifically modified to reflect such differences, since the broad present interpretation of the claim language does not avoid the Huff reference. Huff clearly anticipates placing the detection system within all network elements, while it may not be the intention of the applicant's system to encompass end nodes and network infrastructure as does Huff the claim language simply does not presently overcome the this recitation.

6. Further limitations that are not claimed have been argued by the applicant at page 8 line – page 9 line 12. The applicant states that the system acts only through the "network infrastructure" and not at the end nodes, but these limitations are simply not claimed.

### *Claim Rejections - 35 USC § 102*

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-27 are rejected under 35 U.S.C. 102(b) as being anticipated by Huff et al International Publication No. WO 99/57625 (hereinafter "Huff").

9. Regarding Claim 1: A method of responding to the detection of an intrusion on a network system that provides network services, the network system including one or more attached functions and one or more network infrastructures devices, the method comprising the steps of: a. **using one or more of the network infrastructure devices to monitor** the network system for intrusions (Abstract, Fig 1, 3, pg 5 lines 2-5)

b. upon detection of an intrusion, identifying one or more sources of the intrusion (pg 5 lines 6-9, 12-16, pg 12 line 29 – pg 13 line 3, pg 18 line 27 – pg 19 line 13, pg 20 lines 3-5, pg 21 lines 10-13) Identifying the source of the intrusion occurs two fold within the system of Huff by not only detecting the device on the local network where the issue arises but by tracing the remote location as well.

c. identifying one or more **signal transferring** devices of the one or more network **infrastructure devices** associated with the one or more identified sources (Fig 3-4, pg 4 line 11 – pg 5 line 30, pg 14 line 3 – pg 15 line 10, pg 18 lines 16-26) As depicted by Huff agents associated with intrusion events are identified and send information back to the central server.

d. configuring the identified one or more **signal transferring** devices with one or more policy changes responsive to the detected intrusion (Fig 3-4, pg 4 line 11 – pg 7 line 11, pg 13 lines 10-12, pg 14 lines 6-12, pg 15 lines 3-11, pg 17 lines 14-25, pg 18 lines 1-pg 19 line 25) In response to intrusion detections the system takes actions by changing current monitoring policies or access policies.

10. Regarding Claim 2: The method as claimed in Claim 1 wherein the step of identifying the one or more sources of the intrusions includes the step of identifying a physical address or a logical address of each of the one or more identified sources (pg 8 lines 24-30, pg 11 lines 5-23, pg 12 line 30 – pg 13 line 2, 23-27, pg 18 line 27 – pg 19 line 13, pg 20 lines 3-5, pg 21 lines 10-13)

11. Regarding Claim 3: The method as claimed in Claim 2 wherein the physical address information is a MAC address or the logical address information is an IP address (pg 8 lines 24-30, pg 11 lines 5-23, pg 12 line 30 – pg 13 line 2, 23-27, pg 18 line 27 – pg 19 line 13, pg 20 lines 3-5, pg 21 lines 10-13) As provided by Huff the use of ethernet type networks dictates that for address resolution purposes, which is an inherent functionality of such a network, addresses are stripped from packets which contain both MAC and IP type addresses. Furthermore, as stated since all devices are addressable on the network and the implementation of any such protocol as TCP/IP dictates resolution of such devices occurs via a MAC address associated to an IP address.

12. Regarding Claim 4: The method as claimed in Claim 1 wherein the **one or more of the network infrastructure devices to monitor the network system is** an intrusion detection **device** (pg 4 line 11 – pg 7 line 11, pg 12 lines 15-21, pg 18 lines 1-10, 27-30) Monitoring the network occurs in a distributed manner with all indications sent back to a central server for analysis.

13. Regarding Claim 5: The method as claimed in Claim 4 wherein the intrusion detection **device** is a centralized **network infrastructure device** (Fig 3, pg 4 line 11 –

pg 7 line 11, pg 11 lines 25-30) the intrusion detection function is centralized by the security server that controls actions taken by the distributed agents.

14. Regarding Claim 6: The method as claimed in Claim 4 wherein the intrusion detection **device** is a **plurality of** distributed **network infrastructure devices** (Fig 3, page 8 lines 10-14, 20-30, pg 4 line 11 – pg 7 line 11, pg 17 lines 8-15, pg 20 lines 15-16)

15. Regarding Claim 7: The method as claimed in Claim 4 wherein the intrusion detection **device** is an intrusion detection system (pg 4 line 11 – pg 7 line 11) The functions are correlated together through the central server into a system.

16. Regarding Claim 8: The method as claimed in Claim 1 wherein the step of identifying the one or more **signal transferring** devices associated with the one or more identified sources includes the step of determining the physical address, logical address, or both for each of the identified one or more **signal transferring** devices (pg 8 lines 10-30, pg 11 lines 5-23, pg 12 line 30 – pg 13 line 2, 23-27, pg 18 line 27 – pg 19 line 13, pg 20 lines 3-5, pg 21 lines 10-13) Resolution of addresses in order to send messages and communicate actions must take place via such a path.

17. Regarding Claim 9: The method as claimed in Claim 1 further comprising the step of verifying the identification of the identified one or more sources (pg 5 lines 6-9, 12-16, pg 12 line 29 – pg 13 line 3, pg 18 line 27 – pg 19 line 13, pg 20 lines 3-5, pg 21 lines 10-13) Huff states that agents serve to verify the identity of the source through the steps of tracing.

18. Regarding Claim 10: The method as claimed in Claim 1 wherein the step of configuring the identified one or more **signal transferring** devices with one or more policy changes responsive to the detected intrusion includes the step of configuring the identified one or more **signal transferring** devices to perform one or more functions selected from the group consisting of: blocking complete access to the network services by the identified one or more sources, blocking access by identified logical addresses only, blocking access by an identified access protocol only, limiting bandwidth, limiting exchanges to or from the identified one or more **signal transferring** devices, to or from one or more other network infrastructure devices, or to or from any of the attached functions not identified as an intrusion source (pg 4 line 11 – pg 7 line 11, pg 18 line 1 –pg 19 line 25, pg 22 lines 3-20) The intruder is either disabled through policy changes or is misdirected toward information that cannot be harmed in order to collect further information about the intruder.

and directing all signals exchanged by the identified one or more sources to a honey-pot, an intrusion detection **device**, a monitoring device, or a simulation device (pg 18 line 1 –pg 19 line 25, pg 20 lines 2-8, pg 20 lines 27- pg 21 line 1, pg 21 lines 10-30, pg 22 lines 3-20) The intrusion system directs all information back to the central server which stores information within a database, and also as outlined provides for misdirecting the intruder in order to collect further information.

19. Regarding Claim 11: The method as claimed in Claim 1 wherein the step of configuring the identified one or more **signal transferring** devices with one or more policy changes responsive to the detected intrusion includes the step of configuring the

identified one or more **signal transferring** devices to permit connectivity of the identified one or more sources while dampening the level of activity associated with the identified one or more sources to minimize network harm while permitting analysis and auditing of the identified one or more sources and the gathering of forensic evidence (pg 17 line 18 – pg 19 line 14, pg 21 line 6 – pg 22 line 19) as recited the intruder is misdirected toward data to decrease any possible harm to the network in order to collect data about the attacker.

20. Regarding Claim 12: The method as claimed in Claim 1 wherein the step of configuring the identified one or more **signal transferring** devices with one or more policy changes includes the steps of first configuring a first set of **the identified** one or more **signal transferring** devices with a first set of one or more policy changes, monitoring the network system for intrusions and, upon detection of one or more intrusions related to the intrusions causing the first one or more policy changes, configuring a second set of **the identified** one or more **signal transferring** devices with a second set of one or more policy changes (pg 17 line 18 – pg 19 line 14, pg 21 line 6 – pg 22 line 19) Audit levels may be changed as well as having the attacker misdirected for further examination. Upon detection of further activity from the increase in auditing further actions can be taken by the system to have the attacker disabled or misdirected through policy changes on the specific devices.

21. Regarding Claim 13: The method as claimed in Claim 12 wherein one or more of the one or more **signal transferring** devices of the second set are **signal transferring** devices of the first set (Fig 3, pg 15 lines 3-11, pg 17 lines 8-22, pg 18 lines 1-12, pg 19

lines 1-14) The system has agents on nodes that monitor for intrusions, when an intrusion or suspicious activity is detected the audit level can be increased and upon further inspection if such activity is determined to be inappropriate further action can be taken by the agent.

22. Regarding Claim 14: The method as claimed in Claim 1 wherein the identified one or more **signal transferring** devices are selected from the group consisting of network entry devices and centralized switching devices (Fig 1, page 8 lines 10-14, 20-30, pg 9 lines 12-15, pg 13 lines 24-26) Such devices as servers, hosts, and any other well-known network addressable nodes are anticipated by Huff as containing the agents, such devices as firewalls, VPNs and switches/routers are embodied as network computing devices and thus are anticipated by the present invention.

23. Regarding Claim 15: The method as claimed in Claim 1 wherein the one or more policy changes are configured on one or more ports of one or more of the identified one or more **signal transferring** devices (pg 14 lines 26—pg 15 line 2) Huff provides for configuring agents through associated ports.

24. Regarding Claim 16: a directory service function for receiving address information for attached functions and **network infrastructure** devices; a policy manager function for configuring **one or more signal transferring** devices of the network infrastructure with policies (Fig 4, pg 18 lines 15-26) Huff provides a directory of all monitored devices and there associated enforcement mechanisms. Further, there are means associated with the directory for changing policies and also within the automatic response for implementing and changing policies.

25. Claims 17-27 are further embodiments of the above rejected claims and as such are rejected on the same basis.

***Conclusion***

26. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Applicant is reminded that in amending in response to a rejection of claims, the patentable novelty must be clearly shown in view of the state of art disclosed by the references cited and the objections made. Applicant must show how the amendments avoid such references and objections. See 37 CFR 1.111(c).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Szymanski whose telephone number is 571-272-8574. The examiner can normally be reached on M-F 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on 571-272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TMS

TMS
11/30/2006

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100